UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/052,054	01/17/2002	Timothy W. Kiszely	05655P006	1460

8791 7590 02/14/2006

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
CERVETTI, DAVID GARCIA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 02/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/052,054	KISZELY, TIMOTHY W.	
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 November 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 November 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed November 17, 2005, have been fully considered.

2. Claims 1-24 have been examined, of which, claims 1-10, 14-20, and 23-24 are allowable subject matter, and claims 11-13 and 21-22 remain rejected.

3. Examiner attempted to reach Attorney of Record on February 2, 2006, to discuss allowable subject matter and possible Examiner's Amendment.

Response to Amendment

4. The objection to the drawings is withdrawn.

5. The objection to claim 12 is withdrawn.

6. The following Prior Art was used in this Office Action, Menezes et al. (NPL Handbook of Applied Cryptography, hereinafter Menezes) and Lim (US Patent Application Publication: 2002/0018562).

7. Regarding claim 21, Applicant's arguments regarding the language are not persuasive. The following is the text as it appears on the MPEP C.F.R. 1.75 (e):

> "(e) Where the nature of the case admits, ***as in the case of an improvement***, any independent claim should contain in the following order:
> (1) ***A preamble comprising a general description of all the elements or steps of the claimed combination which are conventional or known***,
> (2) A phrase such as ***"wherein the improvement comprises,"*** and
> (3) Those elements, steps, and/or relationships which constitute that portion of the claimed combination which the applicant considers as the new or improved portion".

It clearly states that the improvement has to have antecedent basis. It is not clear on claim 21 what the improvement is. Is it an improvement upon the Data Encryption Standard? Is it an improvement of an apparatus for performing DES? Is it an improvement of a module within an apparatus performing DES?

8. Regarding claims 11-13, claim 11 simply claims, broadly, performing an XOR on 2 (two) input values and sending the output to a module. Regardless how the input values and the receiving element are labeled, it is still processing of 2 input values to produce an output which is provided to a third element. The traditional DES algorithm provides precisely this teaching, in each iteration of DES, an XOR is performed between two values and the output is provided to a third element (Menezes, pages 250-257).

Allowable Subject Matter

9. Claims 1-10, 14-20, and 23-24 would be allowable.

10. The following is an examiner's statement of reasons for allowance: the prior art of record, Menezes and Lim, does not expressly disclose the claimed arrangement of the elements or using three-input XOR gates. Menezes and Lim are clearly related to the invention, and improve on the Data Encryption Standard, but using other means.

11. The present claimed invention discloses multiple permutation and expansion modules and keys as input to multiple XOR gates and selection functions.

12. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

13. Claim 21 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action.

14. Claim 22 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

15. As allowable subject matter has been indicated, applicant's reply must either comply with all formal requirements or specifically traverse each requirement not complied with. See 37 CFR 1.111(b) and MPEP § 707.07(a).

Claim Objections

16. Claim 21 and 23 are objected to because of the following informalities: "DES" must be spelled out. Appropriate correction is required.

Claim Rejections - 35 USC § 112

17. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

18. Claim 21 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 21 recites the limitation "the improvement comprising" in line 3 of the claim. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

19. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

20. Claims 11-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes, and further in view of Lim.

Regarding claim 11, Menezes et al. teach exclusive-oring, using an exclusive-or gate output from a merged permutation and expansion function module (M.PE), and a sub key block; and sending the output from the exclusive-or gate to a selection function module (pages 250-257). Menezes et al. do not expressly disclose the exact same order of steps or that the permutation and expansion are merged. Lim teaches an 8-cycle Data Encryption Standard implementation (pages 3-5). Therefore, it would have been obvious for such modifications because the same desired effect is acquired. Namely, improve the speed of computing DES. One skilled in the art will recognize that the arrangement is one of many possible arrangements of the logic gates and the permutation and expansion modules, for example, a three-input exclusive or (XOR) gate may be used to replace a pair of two-input XOR gates, and different modules may be combined (Lim, paragraph 104).

Regarding claim 12, the combination of Menezes et al. with Lim teaches the limitations as set forth under claim 11 above. Furthermore, Menezes et al. teach

sending output from the selection function module to a permutation function module (pages 250-257).

Regarding claim 13, the combination of Menezes et al. with Lim teaches the limitations as set forth under claim 12 above. Furthermore, Menezes et al. teach sending output from the selection function module to a second MPE (pages 250-257).

Conclusion

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

22. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

23. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100